Title (en)

METHOD FOR BINDING A TERMINAL APPLICATION TO A SECURITY ELEMENT AND CORRESPONDING SECURITY ELEMENT, TERMINAL APPLICATION AND SERVER

Title (de)

VERFAHREN ZUR BINDUNG EINER ENDGERÄTEANWENDUNG AN EIN SICHERHEITSELEMENT SOWIE ZUGEHÖRIGES SICHERHEITSELEMENT, ENDGERÄTEANWENDUNG UND SERVER

Title (fr)

PROCÉDÉ DE LIAISON D'UNE APPLICATION DE TERMINAL À UN ÉLÉMENT DE SÉCURITÉ ET ÉLÉMENT DE PROTECTION CORRESPONDANT, APPLICATION DE TERMINAL ET SERVEUR

Publication

EP 3282738 A1 20180214 (EN)

Application

EP 16306044 A 20160811

Priority

EP 16306044 A 20160811

Abstract (en)

The invention proposes a method for checking at the level of a service provider (30) if a terminal application (12) comprised in a terminal (10) is entitled to request for a service provided by the service provider (30), a security element (11) cooperating with the terminal (10), the security element (11) containing a first key generated by the terminal application (12) during an enrolment phase, wherein the method comprises: A- Sending, from the service provider (30) to the security element (11), a first message [[[Nonce4MobileApp]Pubkey4app] II Nonce4SIM]Pubkey4SIM, where: - Nonce4MobileApp and Nonce4SIM are data generated by the service provider (30); - Pubkey4app and Pubkey4SIM are respectively the public keys of the terminal application (12) and of the security element (11); B- Decrypting the first message in the security element (11) with the private key of the security element (11); C- Sending from the security element (11) to the terminal application (12) the decrypted first message encrypted by the first key; D- Decrypting in the terminal application (12) the received message with a second key and decrypting the Nonce4MobileApp with the private key of the terminal application (12); E- Sending from the terminal application (12) to the service provider (30) the data Nonce4MobileApp and the Nonce4SIM; F- Checking by the service provider (30) that the received data Nonce4MobileApp and Nonce4SIM correspond to those sent at step -A- and, - if the data correspond, consider that the service provider (30) can trust the terminal application (12) and authorize the service to be executed; - if the data do not correspond, consider that the service provider (30) cannot trust the terminal application (12) and forbid the service to be executed.

IPC 8 full level

H04L 9/32 (2006.01); **H04W 12/08** (2009.01)

CPC (source: EP KR US)

H04L 9/006 (2013.01 - US); **H04L 9/0897** (2013.01 - EP US); **H04L 9/30** (2013.01 - KR); **H04L 9/3271** (2013.01 - EP KR); **H04L 63/083** (2013.01 - US); **H04L 63/0853** (2013.01 - KR US); **H04W 12/03** (2021.01 - KR); **H04W 12/043** (2021.01 - KR); **H04W 12/08** (2013.01 - EP KR US); **H04W 12/35** (2021.01 - KR); **H04W 12/48** (2021.01 - EP KR)

Citation (search report)

- [Y] US 2012084565 A1 20120405 - WITTENBERG CRAIG HENRY [US], et al
- [Y] EP 1513113 A1 20050309 - FRANCE TELECOM [FR]
- [Y] US 2012144201 A1 20120607 - ANANTHA ANOOP [US], et al
- [A] US 2016043872 A1 20160211 - WAJS ANDREW AUGUSTINE [NL], et al

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 3282738 A1 20180214; CN 109792605 A 20190521; EP 3497954 A1 20190619; JP 2019525646 A 20190905; JP 6663537 B2 20200311; KR 20190037306 A 20190405; US 2020092277 A1 20200319; WO 2018029009 A1 20180215

DOCDB simple family (application)

EP 16306044 A 20160811; CN 201780062621 A 20170727; EP 17754287 A 20170727; EP 2017069050 W 20170727; JP 2019507207 A 20170727; KR 20197006626 A 20170727; US 201716324098 A 20170727